Future Generation Computer Systems 89 (2018) 110–125

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Taxonomy and analysis of security protocols for Internet of Things

Ashok Kumar Das [a,*], Sherali Zeadally [b], Debiao He [c]

[a] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[b] College of Communication and Information, University of Kentucky, Lexington, KY 40506, USA
[c] School of Cyber Science and Engineering, Wuhan University, Wuhan 430 072, China

HIGHLIGHTS

- We first discuss essential security requirements that are needed to secure IoT environment. We also discuss the threat model and various attacks related to the IoT environment.
- We then present a taxonomy of security protocols for the IoT environment which includes important security services such as key management, user and device authentication, access control, privacy preservation, and identity management.
- We also present a comparative study of recently proposed IoT-related state-of-art security protocols in terms of various security and functionality features they support.
- Finally, we discuss some future challenges for IoT security protocols that need to be addressed in the future.

ARTICLE INFO

Article history:
Received 10 April 2018
Received in revised form 5 June 2018
Accepted 14 June 2018
Available online 28 June 2018

Keywords:
Access control
Authentication
Identity management
IoT
Key management
Security
Privacy
Sensing devices

ABSTRACT

The Internet of Things (IoT) is a system of physical as well as virtual objects (each with networking capabilities incorporated) that are interconnected to exchange and collect information locally or remotely over the Internet. Since the communication often takes place over the Internet, it is vulnerable to various security threats in an IoT environment. We first discuss essential security requirements that are needed to secure IoT environment. We also discuss the threat model and various attacks related to the IoT environment. We then present a taxonomy of security protocols for the IoT environment which includes important security services such as key management, user and device authentication, access control, privacy preservation, and identity management. We also present a comparative study of recently proposed IoT-related state-of-art security protocols in terms of various security and functionality features they support. Finally, we discuss some future challenges for IoT security protocols that need to be addressed in the future.

1. Introduction

The Internet of Things (IoT) is composed of a large number of things (devices) that are connected through the Internet. A "thing" in the IoT environment can be considered as a person, animal or physical/virtual object that will have a unique identifier (IP address or device ID). IoT devices can transfer sensing information from their surrounding environment via the Internet to some server for further processing. IoT devices can be classified further into two categories:

- *Physical objects:* These can be smartphone, camera, sensor, vehicle, drone, and so on.
- *Virtual objects:* These include electronic ticket, agenda, book, wallet, and so on.

IoT devices can conduct remote sensing, actuating (making an action) and support monitoring capabilities. IoT devices can be made smart enough so that they can operate without any human intervention. The objective of IoT is to provide a strong interaction between the physical world and computer-based systems that can lead to improvements in the economic welfare, and accuracy and efficiency while minimizing human participation.

Fig. 1 [1] shows a generic IoT network architecture in which four different scenarios (e.g., home, transport, community and national) are depicted. Several smart devices, such as sensors and actuators are installed in various applications. All the IoT smart devices are connected to the Internet via trusted Gateway Nodes (GWNs). The information accessed by the IoT devices can be also accessed by

* Corresponding author.
E-mail addresses: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das), szeadally@uky.edu (S. Zeadally), hedebiao@163.com (D. He).

https://doi.org/10.1016/j.future.2018.06.027
0167-739X/

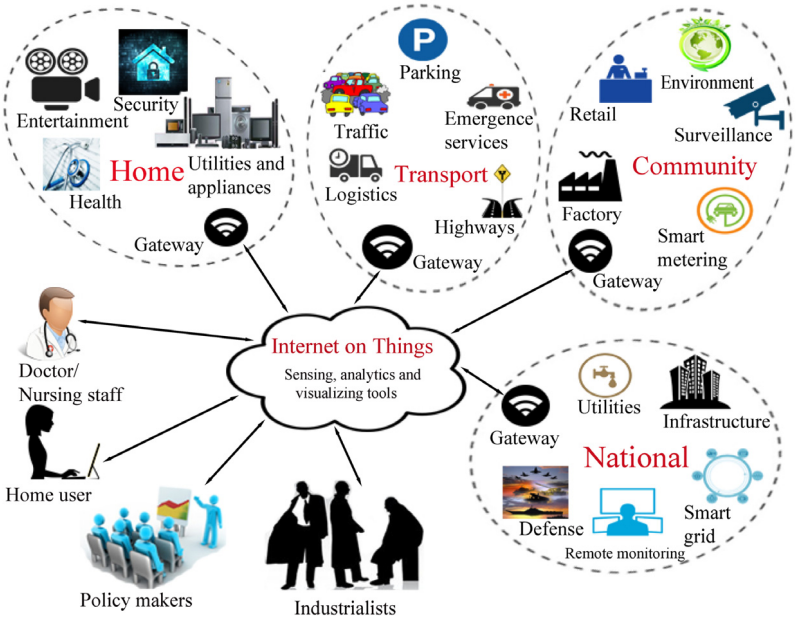

Fig. 1. A generic IoT network architecture [1].

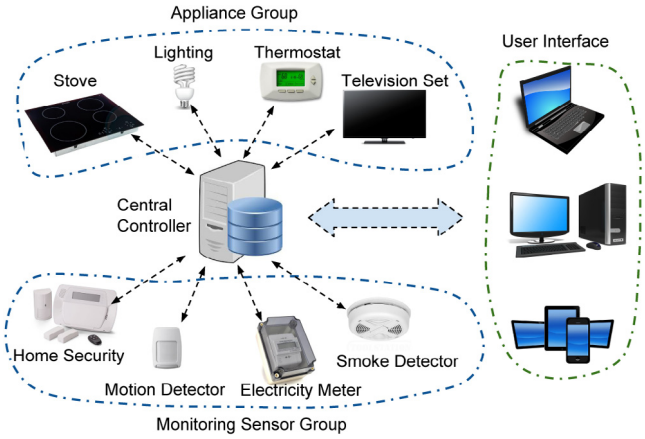

Fig. 2. An IoT-based smart home application [4].

Table 1
IoT units installed based by category (millions of units) [5].

Category	2016	2017	2018	2020
Consumer	3,963.00	5,244.30	7,036.30	12,863.00
Business: cross-industry	1,102.10	1,501	2,132.60	4,381.40
Business: vertical-specific	1,316.60	1,635.40	2,027.70	3,171
Total	6,381.80	8,380.60	11,196.60	20,415.40

various users (e.g., a smart home user in a home application and a doctor in a healthcare application) [2]. Cyber–physical systems such as the smart grid, smart home and intelligent transportation are also parts of IoT ecosystem [3].

Fig. 2 [4] illustrates a generic IoT-based smart home application. The smart devices are deployed into two groups: appliance and monitor. The devices installed in the appliance and monitor groups, known as the agents, communicate with the central controller via wireless communications. A user can control the smart home system by using the user interface. Moreover, the information gathered by any IoT smart device in the monitoring group can be accessed by a user.

Gartner Inc. [5] forecasts that the number of connected IoT devices will reach 20.4 billion by the year 2020. Table 1 shows a summary of the number of IoT units (grouped by category) installed in terms of millions of units in 2016–2017 and also the predicted number of units in 2018 and 2020. In addition to being implemented in various autonomous systems, IoT applications for smart TVs and digital set-top boxes are being used by consumers whereas smart electric meters (also known as smart meters) and commercial security cameras are being widely used in smart grid implementations and businesses respectively [5]. In addition to smart meters, industrial IoT applications and devices, such as manufacturing field devices, real-time location devices for healthcare applications and sensors for electrical generating plants will be the connected things in various businesses and manufacturing plants. It is predicted that cross-industry devices (e.g., Light-Emitting Diode (LED) lighting, physical security systems, and Heating, Ventilation, and Air Conditioning (HVAC) in smart buildings) can take the lead from 2018 onwards since their connectivity is being driven by higher-volume and lower costs. It is worth pointing out that by 2020, cross-industry devices will reach 4.4 billion units, while the vertical-specific devices (e.g., specialized equipment used in hospital operating theaters and tracking devices in container ships) is expected to reach 3.2 billion units.

Table 2
IoT endpoint spending by category (millions of dollars) [5].

Category	2016	2017	2018	2020
Consumer	532,515	725,696	985,384	1,494,466
Business: cross-industry	212,069	280,059	372,989	567,659
Business: vertical-specific	634,921	683,817	736,543	863,662
Total	1,379,505	1,689,572	2,094,881	2,925,787

Since consumers are expected to purchase more IoT devices in the future, business investments are likely to increase in future years. Table 2 summarizes the IoT endpoint spending by category (millions of dollars) [5]. It is expected that, by 2020, hardware spending from both segments can reach around $3 trillion.

We briefly discuss some potential IoT applications below [2,3]:

- *Wearable devices:* Ranging from navigation tools and communication gadgets to fitness trackers and specific health monitoring devices, wearable devices can be used for both